Statement on u-blox's strategy to share security advisories in CSAF format

Topic u-blox introduces machine-readable security advisories and updates in OASIS CSAF format

Document number: UBXDOC-1872205849-50176

Author u-blox Product Compliance team

Document sensitivity: C1-Public

Date 13 October 2026

Version: 2.0

To All u-blox customers

Copying, reproduction, modification, or disclosure to third parties of this document or any part thereof is only permitted with the express written permission of u-blox. The information contained herein is provided "as is" and u-blox assumes no liability for its use. No warranty, either express or implied, is given, including but not limited, with respect to the accuracy, correctness, reliability, and fitness for a particular purpose of the information. This document may be revised by u-blox at any time. For most recent documents, visit www.u-blox.com. Copyright© u-blox AG.

1 Executive Summary

u-blox implements a cyber security management system compliant with EU Cyber Resilience Act's [1] vulnerability management requirements.

u-blox will publish product security advisories, as applicable, starting from the 11th of September 2026, in a structured, machine-readable and human readable format based on the OASIS Common Security Advisory Framework, CSAF [2]. This is a service hosted by our Service Partner VDE CERT.

2 About CSAF

Relevant details of CSAF follow.

- CSAF enables the interoperable and automated exchange of security information concerning products, vulnerabilities, impact status, and available remediation [2].
- CSAF is an internationally developed OASIS standard.
- The CSAF standard is supported by authorities including US CISA[4], EU ENISA [3] and German BSI [6], as well as major technology and industrial companies.
- Its tooling adoption makes it a credible choice for automated vulnerability communication.
- CSAF is recommended in the draft European horizontal standard for CRA vulnerability-handling requirements "prEN 40000-1-3 DRAFT Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling" [3].

3 What u-blox wants to achieve with the adoption of CSAF

u-blox is committed to product security and to improving our compliance with the EU Cyber Resilience Act [1], Regulation (EU) 2024/2847, especially the Vulnerability Handling Requirements established through CRA Article 13, in conjunction with Annex I, Part II. As part of this ongoing commitment, u-blox is enhancing the way in which we communicate security advisories to the public for product vulnerabilities, affected product versions, available mitigations, planned and available security patches, and security updates.

Wherever applicable, our CSAF Security Advisories will serve the purposes and provide the elements as follows.

- The security advisories identify and document applicable vulnerabilities for our products and services.
- Each security advisory will be treated as the authoritative source of the latest version including a revision history.

- They help to explain the security impact and severity assessment.
- They identify the affected products, product versions and firmware versions.
- They list the status of individual products, for example, affected, not affected, fixed or under investigation.
- Security advisories reference relevant CVE identifiers and other supporting information, where available.
- They contain information about available mitigations or workarounds.
- They include references to available security patches, firmware updates or updated software packages.
- They facilitate the sharing and speed up distribution of vulnerability information.
- They contain publication and revision history.

4 Recommendations for u-blox customers

We recommend that customers begin preparing their asset inventories, CSAF ingestion capabilities, and internal vulnerability-management workflows, so that CSAF Security Advisories can be assessed and acted upon efficiently by your PSIRT (Product Security Incident Response Team).

To benefit from our Security Advisory publication service and incorporate the information into your own vulnerability-management processes, we recommend that you do the following.

1. **Learn more on CSAF.**
   - CSAF Homepage [2]
   - CSAF Guidance available from other sources, e.g. BSI [6]
   - Use the CSAF downloader Tool to fetch and read security advisories
2. **Regularly poll for Security Publications and Security Advisories.**
   Human readable HTM Version of CSAF-Feed of security advisories are available at:
   CSAF Security Advisories Index (TLP:WHITE)
3. **Subscribe to our CSAF security advisory service.**
   Establish automated systems that poll our security advisories from our CSAF distribution point published in the u-blox security.txt: www.u-blox.com/.well-known/security.txt
4. **Do not rely on email notifications.**
   Security publications and advisories will only be made available in CSAF format through the u-blox CSAF distribution point and in a human readable version. Email notifications will not be used for this purpose anymore.
5. **Integrate CSAF into your vulnerability-management process.**
   Configure your vulnerability-management, product-security, or asset-management solution to retrieve and process our CSAF documents automatically, as CSAF is designed to support automated assessment workflows.
6. **Maintain an accurate inventory of u-blox components integrated into your products.**
   Record the hardware and firmware/software versions of the u-blox components used in your products or systems. This allows CSAF product identifiers and affected-version information to be matched against our deployed product inventory.
7. **Assess the applicability of each advisory.**
   u-blox customers shall determine whether the u-blox components (and versions) identified in an advisory are incorporated into their products, deployed in their systems, and/or in

turn supplied to their customers. Customers remain responsible for evaluating each advisory in the context of their own product architecture and intended use.

8. **Evaluate and deploy security updates, if needed.**
   u-blox customers shall review available patches, firmware updates, recommended mitigations and installation instructions from u-blox. Customers shall validate and deploy security updates within a timeframe proportionate to the applicable cybersecurity risk and the operational requirements of their product or system.
9. **Retain compliance evidence.**
   Customers shall retain the relevant CSAF advisory, their applicability assessment, resulting risk decisions, update or mitigation records, test evidence, and deployment status as part of their product cybersecurity and technical documentation.
10. **Inform downstream customers where required.**
    Customers who integrate u-blox components into a product with digital elements and/or distribute them further shall incorporate applicable vulnerability and remediation information into their own vulnerability-management and customer-notification processes. Receiving a u-blox advisory does not automatically fulfil a customer's own CRA obligations as a manufacturer, importer, or distributor.

For questions concerning a specific advisory please contact support@u-blox.com.

Details on our vulnerability disclosure process are available at:
https://www.u-blox.com/en/security-management.

5 References and Supporting Guidance

[1] CRA REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024
[2] OASIS Common Security Advisory Framework (CSAF) | Homepage
[3] EN 40000-1-3 Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling
[4] CSAF/csaf_files/OT/white at develop · cisagov/CSAF · GitHub
[5] GitHub - gocsaf/csaf: Tools to download or provide CSAF (Common Security Advisory Framework) documents. · GitHub
[6] BSI - Common Security Advisory Framework (CSAF) Guidance